Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy and Know Your Customer (KYC) Policy

Aladdin Fintech Company Limited (the "**Company**") has put in place an Anti-Money Laundering /Counter-Terrorist Financing Policy and a Know Your Customer Policy (collectively, the "**AML/KYC Policies**") based on recommendations made to and approved by its Board for the operation of the Company's token sale and token listing (the "**Token Sale**"). The AML/KYC Policies are revisited periodically and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing. All senior management and employees of the Company are required to acknowledge and be familiar with the AML/KYC Policies.

The AML/KYC Policies are designed to lay down a framework to:

a. prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;

b. enable the Company to know/understand its customers, clientele, contributors, business associates, and other contacts with which the Company has any financial dealings with (collectively, "**Dealing Entities**") in relation to the Company and their financial background and source of funds better, which in turn would help it to manage its risks prudently;

c. put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and

d. equip employees of the Company with the necessary training and measures to deal with matters concerning AML/KYC procedures and reporting obligations.

THE POLICIES

RISK-BASED APPROACH

The Company shall adopt and maintain a Risk-Based Approach ("**RBA**") towards assessing and containing the money laundering and terrorist financing risks to the Company arising from the use of the services on the Company. The guidelines are as follows:

a. Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the Dealing Entities or persons associated with the entities does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations.

b. For the purpose of risk categorization of Dealing Entities, the relevant information shall be obtained from the Dealing Entities at or before the time of entering into the transaction or commencement of business relationship.

c. The risk categorization process for different types of Dealing Entities may take into account the background of the Dealing Entities, nature of business activity, location of Dealing Entities / activity

and profile of participants of the Company, country of origin, sources of funds, mode of payments, volume of turnover, social and financial background.

d. The outcome of the risk categorization process shall be decided based on the relevant information provided by the Dealing Entities at the time of commencement of business relationship.

e. Enhanced due diligence would be required for higher risk Dealing Entities, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by the Company at its sole and absolute discretion.

f. The Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the Dealing Entities in compliance with the relevant legislations in place.

g. If the Company deems necessary, the Company may appoint a Third-Party AML/KYC specialist screening firm to ensure compliance with prevailing regulations and the Company's policies. The Company must be satisfied that such third party is adequately regulated, supervised or monitored, and has measures in place for compliance with participant due diligence and record-keeping requirements in line with the requirements and obligations under the applicable regulations, and that the third party is not based in a country or jurisdiction assessed as high-risk.

1. PARTIPATION AT THE TOKEN SALE AND LISTING:
    a. Establishing and maintaining risk-based due diligence, identification, verification and KYC procedures, including enhanced due diligence for those Dealing Entities presenting higher risk, such as Politically Exposed Persons (PEPs).
    b. The Company should not allow the participation from any Dealing Entities in fictitious name or on behalf of other persons whose identity has not been disclosed or cannot be verified.
    c. The maintenance of appropriate records for the minimum prescribed periods, but also subject to the Company's privacy policy.

2. INTERNAL CONTROLS
    a. The Company will develop and implement internal controls for the purpose of ensuring that all of its operations comply with AML/KYC legal requirements and that all required reports are made on a timely basis. Some of those internal controls are listed within this document and may include, but are not limited to, the Customer Identification Program, the Suspicious Activity Reporting system, and the required reports on the Policies' effectiveness to the Board.

3. CUSTOMER IDENTIFICATION PROGRAM
    a. The Customer Identification Program is to be carried out at the following stages: (i) prior to committing to sell or list any tokens through the Company at the Token Sale; (ii) before or during the carrying out of any financial transaction; and (ii) when there is any doubt about the authenticity/veracity or the adequacy of the previously obtained Dealing Entities' identification data.
    b. The Company will require Dealing Entities to provide proof of identification.
    c. When there shall be any suspicion of money laundering or terrorism financing activities, or where there shall be any doubt about the adequacy or veracity of previously obtained

Dealing Entities' identification data, the due diligence measures shall be reviewed, including verifying again the identity of the Participant and obtaining information regarding the purpose and intended nature of the business relationship with the Company.

4. PROOF OF IDENTIFICATION:
    a. For natural persons, sufficient identification data shall be obtained to verify:
        - Full name
        - Date of birth
        - Nationality/ Citizenship
        - Country of birth
        - City or town of birth "Government-issued identification number (where applicable): i.e. national identity number or Passport number"
        - Gender
        - Residential address
            - Verification of address is required by obtaining a copy of acceptable address proof document (one or more, at the discretion of the Company) issued in the 3 months prior to establishing an account. The document must carry the Participant's name and address.
        - Permanent address (if different from residential)
        - Correspondence address (if different from residential)
        - Identification and Verification of authorized agents (e.g. any power of attorney of the account)
    b. For other legal entities, sufficient documentation shall be obtained to verify:
        - Name
        - Government-issued identity documents (for connected parties)
        - Address proof document for connected parties (issued within 3 months of date received)
        - Certificate of Incorporation/ or Certificate of Registration
        - The Company Search Report/ or Certificate of Incumbency (COI)
        - M&AA/ Constitution/ Articles of Incorporation/ By-Laws
        - Organization chart for ownership structure
        - The standing of any person purporting to act on behalf of the legal entity
        - The ownership and control structure of the legal entity, and to determine who are the natural persons who ultimately control the legal entity
        - The Identification Data of the natural persons who ultimately control the legal entity (see above)
        - List of key controllers
        - Trust Deed (If any)
        - If partial Trust Deed is provided, this should include the front page of the initial trust deed and the last pages of the latest Deed, which should contain the following information;
        - Appointment of current Trustees,
        - Full name of the Trust and Trading As Name, and
        - Trustees' signature (If any)
        - Declaration of Trust (If any)
        - Foundation Charter (If any)

- Declaration of Foundation (If any)

c. For other legal entities, sufficient documentation may (at the Company's determination) be obtained to verify:
   - Latest Annual Report
   - Partnership agreement (Full)
   - Partnership agreement (Partial) or Latest Annual Report
   - Evidence from reliable public sources e.g. extract of latest listed stock register, indicating that the Participant is listed on a stock exchange in a FATF member country

5. VERIFICATION
   a. Documents used for participation at the Token Sale must be verified prior to the acceptance of the Dealing Entities as a listing entity of certain token. Verification of identity may require multi-factor authentication, layered security and other controls to ensure a meaningful user identity confirmation process based on account size or other factors.
   b. The following are a list of documents that the Company will require from Dealing Entities for verification:
      - Identity document (such as passport copy);
      - Source of funds information (which may include bank statements and previous trading portfolio);
   c. The following are examples of verification methods the Company may use but is not an exhaustive list of the documents that the Company may request:
      - Obtaining proof of address, such as a copy of a utility bill or bank statement from the account holder.
      - Comparing the identifying information with information available from a trusted third-party source, such as a credit report from a consumer-reporting agency.
      - Analyzing whether there is logical consistency between the identifying information provided, such as the Dealing Entities' name, street address, postal code, telephone number, date of birth, and social security number (logical verification).
      - Utilizing knowledge-based challenge questions.
      - Utilizing complex device identification (such as "digital fingerprints" or IP geo-location checks).
      - Obtaining a notarized or certified true copy of an individual's birth certificate for valid identification.

6. SUSPICIOUS PARTICIPATION AND ACTIVITY REPORTS
   a. For the purpose of the Policies, a "Suspicious Transaction" means a transaction or attempted transaction, which to a person acting in good faith:
      - gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
      - appears to be made in circumstances of unusual or unjustified complexity;
      - appears to have no economic rationale or bona fide purpose; and
      - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

b. Internal controls will be implemented so that a monitoring system is in place to reasonably detect any Dealing Entities who appears to be conducting or have conducted Suspicious Transaction. When a Suspicious Activity is detected, the Company's senior management will make the decision as to whether the transaction meets the definition of Suspicious Transaction or activity and whether any filings with law enforcement authorities should be filed. The Company reserves the right to report Suspicious Transactions or activity to law enforcement authorities at its sole discretion.
c. The Company will maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing. The Company may inform the Company's Board of the filing and the underlying transaction.

7. MAINTAINING RECORDS
   a. Reasonable procedures for maintaining records of the information used to verify a person's name, address and other identifying information submitted for the purposes of utilizing the services on the Company are required under this Policy. The following are required steps in the record keeping process:
      - The Company is required to maintain a record of identifying information provided by the Dealing Entities.
      - Where the Company relies upon a document to verify identity, the Company must maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain.
      - The Company must also record the methods and result of any additional measures undertaken to verify the identity of the Dealing Entities.
      - The Company must record the resolution of any discrepancy in the identifying information obtained.
      - All transaction and identification records will be maintained for as long as reasonably necessary for the purpose of operating the Platform and to comply with applicable regulations.
   b. All information collected from the Participants will be subject to the Company's privacy policy, which is announced from time-to-time.
   c. For citizens from European Economic Area (the "**EEA**"), we shall only obtain and record your information for the purpose of this policy and our privacy policy. Please refer to our privacy policy on how your information may be used.